

## UNITED STATES DISTRICT COURT

for the  
Eastern District of Missouri

FILED

MAR - 4 2015

U.S. DISTRICT COURT  
EASTERN DISTRICT OF MO  
ST. LOUIS

In the Matter of the Search of  
 Matthews Manufacturing, Incorporated, 41 Branch Street, St. Louis, MO 63147,  
 further described as three story brown brick building with a painted blue stripe  
 between the second and third stories. The word "Matthews" is shown vertically  
 on the southwest corner of the building, and a blue awning is painted with a  
 white "41" which faces south. The structure has two green doors which face  
 south. On the north side of the building is a brown metal structure with a white  
 garage - like door.

Case No. 4: 15 MJ 3062 NCC

## APPLICATION FOR A SEARCH WARRANT

I, Christopher Thesing, a federal law enforcement officer or an attorney for the government  
 request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

Matthews Manufacturing, Incorporated, 41 Branch Street, St. Louis, MO 63147, further described as three story brown brick building with a painted blue stripe  
 between the second and third stories. The word "Matthews" is shown vertically on the southwest corner of the building, and a blue awning is painted with a white  
 "41" which faces south. The structure has two green doors which face south. On the north side of the building is a brown metal structure with a white garage - like  
 door.

located in the EASTERN District of MISSOURI, there is now concealed

See Attachments A and B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.


The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. Section 1341	Mail Fraud
18 U.S.C. Section 1343	Wire Fraud

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE


- ☒ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested  
 under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
 Applicant's Signature  
 Special Agent Christopher Thesing  
 DOD/Office of the Inspector General/DCIS  
 Printed name and title

Sworn to before me and signed in my presence.

Date: 3/4/2015

City and state: St. Louis, MO

  
 Judge's signature

Honorable Noelle C. Collins, U.S. Magistrate Judge

Printed name and title

AUSA: Hal Goldsmith

**AFFIDAVIT**

I, Christopher Thesing, being duly sworn, hereby depose and state as follows:

I am employed as a Special Agent with the United States Department of Defense (DoD), Office of the Inspector General (OIG), Defense Criminal Investigative Service (DCIS), St. Louis, Missouri, and have been so employed since August 2012. Prior to my employment with DCIS, I was employed as a Special Agent with the Special Inspector General for Afghanistan Reconstruction (SIGAR) From March 2011 to August 2012. From July 2009 until June 2010, I served as a Criminal Investigator with the District of Columbia Government, Office of Integrity and Oversight. As a Criminal Investigator, I investigated crimes related to government corruption and employee misconduct. From August 2006 until July 2009, I held the position of Special Agent with the Maryland Office of the State Prosecutor. As a Special Agent, I investigated incidents involving governmental corruption, bribery, theft, and embezzlement. I hold the Certified Fraud Examiner designation.

This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter. This affidavit is being submitted in support of an application for a search warrant for Matthews Manufacturing, Incorporated located at 41 Branch Street, St. Louis, MO 63147, further described in Attachment A; in order to obtain evidence of violations of Federal Law, specifically: Title 18, United States Code, Sections 1341 (Mail Fraud) and 1343 (Wire Fraud).

**BACKGROUND**

Since January 2015, I, along with the Naval Criminal Investigative Service (NCIS), have been investigating the business known as Matthews Manufacturing, Incorporated (MMI), its principal, Matthew Alexander, and employees for mail and wire fraud violations.

MMI was founded in 1996, and Matthew Alexander (Alexander) serves as the company's President. According to MMI's website, and based on information obtained during this investigation, MMI is a Veteran Owned, ISO Certified sheet metal fabricating company. The company has served as a prime contractor for multiple United States Government contracts. MMI's offices and sole manufacturing facility are located at 41 Branch Street, St. Louis, Missouri.

The Federal Acquisitions Regulation (FAR) is jointly issued by the DoD, General Services Administration (GSA), and the National Aeronautics and Space Administration (NASA) for use by executive agencies in acquiring goods and services. The FAR outlines the rules and regulations for the Government procurement process. Both Government contractors and their sub-contractors are required to abide by the FAR and any additional rules set forth by their individual contracts with the Government.

The DoD depends upon its U.S. contractors to provide a vast array of equipment and services used by the military. The DoD employs contract administration personnel to review contractor production systems, evaluate progress and inspect defense articles procured by the DoD. In order to ensure contractors meet their contractual obligations, DoD contract administration personnel often demand, per the authority of the contracts, that prime contractors maintain copies of certificates of conformance, compliance or origins for their subcontractors.

DoD contractors must utilize the secure web based system for electronic invoicing, receipt, and acceptance known as Wide Area Work Flow (WAWF). WAWF allows government vendors to submit and track invoices and receipt/acceptance documents over the web and allows government personnel to process those invoices in a real-time, paperless environment. WAWF is

the only acceptable electronic system for submitting requests for payment (invoices and receiving reports) under DoD contracts.

**F414 HIGH PRESSURE TURBINE MODULE SHIPPING CONTAINER**

On June 2, 2010, The Defense Logistics Agency (DLA) awarded contract, SPRPA1-10-C-Z063, to MMI for the construction of fifty-seven (57) F414 High Pressure Turbine Module Shipping Containers. The contract was valued at \$293,480.88. The F414 High Pressure Turbine is a critical engine component for the F/A-18 Super Hornet aircraft. Shock mounts are critical components utilized in the construction of F414 High Pressure Turbine Module Shipping Containers, and according to the contract specifications:

*Each shock mount shall be marked with its manufacturing cure date (month and year) permanently molded in the top of the mount material so as to be plainly visible when the mount is installed. If mount configuration makes this impossible; the cure date shall be stamped on the top surface of the flexing element using white waterproof ink conforming to the TT-I-1795. Shock mounts shall be no older than one year old when installed in the container.*

Between March 1, 2011 and April 19, 2011, MMI received 200 shock mounts for the F414 High Pressure Turbine Module Shipping Container from the manufacturer of the shock mount, Dow-Elco. According to invoices provided by Dow-Elco 158 of the shock mounts had a cure date of February of 2011 and 42 of the shock mounts had a cure date of April of 2011. Each F414 High Pressure Turbine Module Shipping Container contains four (4) shock mounts.

The shock mounts contain two markings which indicate the shock mount's cure date. A white alpha-numeric marking indicating part number, manufacturer, and cure date:



And a marking molded into the rubber of the shock mount indicating the cure month and year. The molded marking appears similar to the following:



11

To decode the molded marking; each quadrant represents a quarter of the year, and each dot indicates the number of months in that quarter of the year. The number indicates the manufacturing year. The example above would be interpreted as February of 2011.

On April 30, 2012, MMI sent their first article test (FAT) sample of the F414 High Pressure Turbine Module Shipping Container. The FAT is tested by DLA engineers to ensure the F414 High Pressure Turbine Module Shipping Container meets all contract specifications.

On March 19, 2014, MMI shipped nine (9) F414 High Pressure Turbine Module Shipping Containers to the DLA Distribution center in Jacksonville, FL, certified compliance via WAWF, and were paid.



On November 10, 2014, MMI shipped four (4) F414 High Pressure Turbine Module Shipping Containers to the DLA Distribution center in Jacksonville, FL, certified compliance via WAWF, and were paid.

On November 14, 2014, MMI shipped four (4) F414 High Pressure Turbine Module Shipping Containers to the DLA Distribution center in Jacksonville, FL, certified compliance via WAWF, and were paid.

On December 2, 2014, MMI shipped three (3) F414 High Pressure Turbine Module Shipping Containers to the DLA Distribution center in Jacksonville, FL, certified compliance via WAWF, and were paid.

On December 8, 2014, MMI shipped three (3) F414 High Pressure Turbine Module Shipping Containers to the DLA Distribution center in Jacksonville, FL, certified compliance via WAWF, and were paid.

During December 2014, a Defense Contract Management Agency (DCMA) Quality Assurance Representative (QAR) visited the MMI St. Louis, Missouri facility. During his visit, the QAR noticed a white plastic bin containing 15 shock mounts. The DCMA QAR noticed the white alpha-numeric markings on the shock mounts was tacky to the touch. The QAR asked the MMI Quality Assurance Specialist (QAS), Larry Maxwell (Maxwell), if the alpha-numeric marking had recently been placed on the shock mount. Maxwell stated the shock mounts had recently been provided by Alexander who retains the parts in his office, and Maxwell did not know of any discrepancies. The QAR noted the white alpha-numeric label stated the part was produced in 2014, while the rubber molded marking indicated the part was produced in February of 2011. The QAR confronted Alexander, who denied any wrongdoing. The QAR photographed the questionable shock mounts.

On January 27, 2015, I telephonically interviewed Ray Olea (Olea), Dow-Elco Quality Manager, and provided him with pictures of the shock mounts taken by the QAR at MMI during December, 2014. Olea stated the white alpha-numeric markings on the shock mounts were “obvious forgeries”. He stated the molded markings on the shock mounts are the true manufacturing dates.

On January 27, 2015, NCIS Special Agents located one of the MMI manufactured F414 High Pressure Turbine Module Shipping Containers at Naval Air Station Jacksonville, FL. On two of the four shock mounts, the white alpha-numeric markings indicated the shock mounts were produced in 2013, but the molded cure dated markings indicated the shock mounts were produced in 2011.

On January 30, 2015, NCIS Special Agents located 17 MMI manufactured F414 High Pressure Turbine Module Shipping Containers at Naval Air Station Lemoore, California. Six (6) of the containers contained alpha-numeric white labels which indicated the shock mounts were produced in 2013, although the rubber molded cure dates indicated the shock mounts were produced in February 2011. Eleven (11) of the F414 High Pressure Turbine Module Shipping Containers were missing the cure dates on the white alpha-numeric labels, although the molded cure dates indicated the shock mounts were produced between 2000 and 2009.

#### **V-22 CONVERSION ACTUATOR CONTAINER**

On May 18, 2010, the United States Government awarded contract SPRPA1-10-C-W043 valued at \$109,491.69 to MMI for the construction of 22 V-22 Conversion Actuator Containers. A conversion actuator is a critical component which rotates the engine and rotor nacelles on the United States Marine Corps’ V-22 Osprey aircraft. Each of these containers was required to incorporate 4 shock mounts.

In December of 2014, MMI sent their V-22 Conversion Actuator Container First Article Test to Karen Ann McDonnell (McDonnell), Mechanical Engineer for the Naval Air Systems Command (NAVAIR). McDonnell noticed the cure dates on the 4 Dow-Elco shock mounts did not match. McDonnell stated Dow-Elco is a common producer of shock mounts and she was very familiar with their appearance. McDonnell advised upon viewing the shock mounts in the V-22 Conversion Actuator Container, she immediately recognized the stenciled font used for the Dow-Elco manufacture date had a different appearance than those she had seen in the past. She inspected the molded marking on the four shock mounts and found the cure dates did not match.

According to the contract, shock mounts are not to be older than one (1) year, and each mount must be produced on the same date to ensure structural integrity. According to McDonnell, the rubber on each shock mount begins to degrade after manufacture and if the mounts in a container have different cure dates they will not dampen movements appropriately, which can affect the integrity of the container and the equipment the container was built to protect. She stated improper shock mounts could damage the equipment and ultimately cause the equipment to fail in the field.

#### **V-22 ROTOR BLADE SHIPPING CONTAINER**

In February 2015, DLA terminated for default MMI's contract to produce V-22 Rotor Blade Shipping Containers, and Alexander has been made aware of a potential issue with his company's shock mounts.

#### **SUMMARY**

In summary, your Affiant believes, based upon the information and evidence set forth above, that there is probable cause to believe that MMI, its President and employees have manufactured, shipped and certified DOD contracted containers containing out of date and



altered shock mounts in violation of the mail and wire fraud statutes. Based upon the investigation, the only shock mounts MMI received from its supplier Dow-Elco were 200 during 2011. During 2013 through 2014, MMI shipped twenty-five DOD ordered containers each containing four of these Dow-Elco 2011 manufactured shock mounts, which shock mounts had been falsely altered to appear as if they were manufactured during 2013-2014. Based upon these seized containers, it is believed that there are approximately 100 of the Dow-Elco 2011 manufactured shock mounts remaining at the MMI St. Louis facility, possibly with altered and false manufacture dates. During December, 2014, DCMA inspectors observed a quantity of Dow-Elco 2011 manufactured shock mounts which appeared to have their manufacture dates altered within the MMI St. Louis facility. MMI is also required per DOD guidelines to retain records related to the acquisition, production, and distribution of their container products. Based upon information and evidence to date, it is believed that MMI has submitted false certifications to DOD relative to the above-referenced shipping containers and their component shock mounts through the DOD internet based system. There is probable cause to believe that records, shock mounts, and other materials evidencing MMI's fraud scheme are currently contained within the MMI St. Louis facility.

#### **TECHNICAL TERMS**

Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP

address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

#### **COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

As described in Attachment B, this application seeks permission to search for records that might be found at Matthews Manufacturing, Incorporated, 41 Branch Street, St. Louis, MO 63147, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

*Probable cause:* I submit that if a computer or storage medium is found at Matthews Manufacturing, Incorporated, 41 Branch Street, St. Louis, MO 63147, there is probable cause to

believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.  
  
Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space-that is, in space on the storage medium that is not currently being used by an active file-for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. As stated above, MMI must utilize the secure web based system for electronic invoicing, receipt, and acceptance known as Wide Area Work Flow (WAWF). Furthermore, the DCMA QAR revealed that Matthew Alexander corresponds electronically through the internet (global network of computers and other electronic devices that communicate with each other) with DCMA. There is reason to believe that there is a computer system currently located at Matthews Manufacturing, Incorporated, 41 Branch Street, St. Louis, MO 63147.

- d. SA Steven Wattles has been employed with the Defense Criminal Investigative Service (DCIS) since 1994. SA Wattles is a DCIS Seized Computer Evidence Recovery Specialist (SCERS), and he was trained in computer forensics at the Federal Law Enforcement Training Center (FLETC), Brunswick, Georgia. SA Wattles has received advanced training in the area of the execution of search warrants involving computers and related equipment, electronic data preservation, and the recovery, documentation, and authentication of computer evidence. SA Steven Wattles informed your affiant that conducting a search of a computer system, documenting the search, and making evidentiary and discovery copies is a lengthy process. It is necessary to determine that no security devices are in place that could cause the destruction of evidence during the search; in some cases it is impossible even to conduct the search without expert technical assistance. Since computer evidence may be extremely vulnerable to tampering or to destruction through error, electrical outages, and other causes, removal of the system from the premises will assist in retrieving the records authorized to be seized, while avoiding accidental destruction or deliberate alteration of the records. SA Wattles also stated that whether records are stored electronically or on a hard drive or otherwise, even when they purportedly have been erased or deleted, they may still be retrievable. SA Wattles is familiar with the methods of restoring lost data commonly employed by computer users, and has used those methods himself. He stated that should such data retrieval be necessary, it is time consuming.
- e. SA Wattles stated the accompanying software must also be seized, since it may be impossible without examination to determine that it is standard, commercially

available software. It is necessary to have the software used to create data files and records in order to read the files and records. In addition, without examination, it is impossible to determine that any electronic media purporting to contain a standard commercially available software program has not been used to store records instead.

- f. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

*Forensic evidence:* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium at Matthews Manufacturing, Incorporated, 41 Branch Street, St. Louis, MO 63147, because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a



file (such as a paragraph that has been deleted from a word processing file).

Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.
- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

*Necessity of seizing or copying entire computers or storage media:* In most cases, a thorough search of premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. *The time required for an examination:* As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. *Technical requirements:* Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. *Variety of forms of electronic media:* Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

*Nature of examination:* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media

that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

Matthews Manufacturing, Incorporated is a functioning company that conducts legitimate business. The seizure of the Company's computers may limit the Company's ability to conduct its legitimate business. As with any search warrant, I expect that this warrant will be executed reasonably. Reasonable execution will likely involve conducting an investigation on the scene of what computers, or storage media, must be seized or copied, and what computers or storage media need not be seized or copied. Where appropriate, officers will copy data, rather than physically seize computers, to reduce the extent of disruption. If employees of the Company so request, the agents will, to the extent practicable, attempt to provide the employees with copies of data that may be necessary or important to the continuing function of the Company's legitimate business. If, after inspecting the computers, it is determined that some or all of this equipment is no longer necessary to retrieve and preserve the evidence, the government will return it.

### **CONCLUSION**

I submit that this affidavit supports probable cause for a warrant to search Matthews Manufacturing, Incorporated located at 41 Branch Street, St. Louis, MO 63147, further described in Attachment A and seize the items described in Attachment B. All of which constitute

evidence, fruits, and instrumentalities of violations of Federal Law, specifically: Title 18, United States Code, Sections 1341 (Mail Fraud) and 1343 (Wire Fraud).



## **ATTACHMENT A**

### **PROPERTY TO BE SEARCHED**

The Property to be search is described as Matthews Manufacturing, Incorporated, 41 Branch Street, St. Louis, MO 63147, further described as three story brown brick building with a painted blue stripe between the second and third stories. The word “Matthews” is shown vertically on the southwest corner of the building, and a blue awning is painted with a white “41” which faces south. The structure has two green doors which face south. On the north side of the building is a brown metal structure with a white garage – like door.





**ATTACHMENT B**

**ITEMS TO BE SEIZED**

The Following records and items dated from January 1, 2010 to the current, located at Matthews Manufacturing, Incorporated, 41 Branch Street, St. Louis, MO 63147, in the Eastern District of Missouri, to include, but are not limited to originals, photocopies, drafts, notes, and computer records. These records and items constitute evidence, fruits and instrumentalities of the violations of the United States Code Title 18 §1341 (Mail Fraud), 1343 (Wire Fraud).

The term "document(s)" means all written or printed matter of any kind, formal or informal, including the originals and all non-identical copies thereof, whether different from the original by reason of any notation made on such copies or otherwise, in the possession, custody or control of the company, wherever located, including, but not limited to, papers, correspondence, electronic mail, memoranda, notes, diaries, statistical materials, letters, telegrams, minutes, contracts, reports, studies, checks, statements, receipts, returns, summaries, pamphlets, books, drawings, interoffice and intra-office communications, offers, notations of any sort of conversations, telephone calls, meetings or other communications, bulletins, credit matters, telefax materials, invoices, worksheets and all drafts, alterations, modifications, changes and amendments of any nature or kind of the foregoing and all graphic and aural records or representations of any kind, including but not limited to, sound recordings, motion pictures and any electronic, mechanical or electrical recordings or representations of any kind, including, but not limited to, tapes, cassettes, discs, recordings and films.

1. Any and all documents relating to or corresponding with Department of Defense contracts awarded to Matthews Manufacturing, Incorporated; to include but not be limited to: request for quotations, quotes, purchase orders, solicitations, invoices, shipping records, receiving records, material quotes, correspondences, electronic correspondences, receipts, memorandums, letters, diaries, work papers, ledgers, billing statements, records of payments received or expended, and accounts receivable journals.
2. Altered or defaced shock mounts
3. Equipment to alter or deface shock mounts
4. Any and all records related to communications between employees of Matthews Manufacturing, Incorporated and their supplier Dow-Elco.
5. Business Records which reflect documents of incorporation, partnership agreements, corporate meeting minutes, tax records and annual reports.
6. Personnel, payroll and training records which reflect identity of officers and employees, home addresses and phone numbers, dates of employment and title and/or position.

7. Any and all information and/or data, pertaining to records set forth above under numbers 1 through 6, inclusive, stored in the form of magnetic or electrical coding on computer media or on media capable of being read by a computer or with the aid of computer related equipment. This media includes, but is not limited to, hard drives, personal digital assistants (PDAs), compact flash cards, external media, removable hard disks, optical drives, recordable CD-roms, DVDs, tapes, and any other media which is capable of storing magnetic or optical data.
8. Computer codes and programs, computer software, instructional manuals, operating instructions and sources of information manuals, operating instructions and sources of information, to the extent that they are necessary to extract and copy any of the information set forth above.
9. If a determination is made during the search by the Special Agent assigned, the computer aspect of this search, that by extracting and copying information contained in the computer or computer system, and related computer equipment and storage devices, that the recreation of the exact computer environment at the premises being searched, cannot be assured in accordance with good evidence processing practices, the following items are included for seizure:
  - a. Computers and computer equipment, including processing unit and circuit boards, attached or unattached to the computer;
  - b. Magnetic storage media such as hard drives and magnetic computer tap, and magnetic storage devices, such as read/write devices and read only devices, whether internal or external;
  - c. Photo optical storage media, including, but not limited to, compact disk type storage devices which are forms of storage devices for computer readable information;
  - d. Computer peripheral devices attached or unattached to the computer, including computer monitors, printers, keyboards, routers, or other physical devices which serve to transmit or receive information to or from a computer;
  - e. Documents which serve the purpose of explaining the way the computer hardware programs and data are used, including manuals for computer equipment and software, printouts of computer programs, data files or other information which have been or continue to be stored electronically or magnetically in a computer system; and
  - f. Memory telephones, automatic dialing devices, telephone answering machines, or any other electronic or digital used for the storage of names, addresses, and telephone numbers.